UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/000,154	10/23/2001	Koteshwerrao S. Adusumilli	42P12318	2225

45209 7590 01/12/2011

MISSION/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/12/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KOTESHWERRAO S. ADUSUMILLI
and
JOHN B. ABJANIC

Appeal 2009-006838
Application 10/000,154
Technology Center 2400

Before CARLA M. KRIVAK, THOMAS S. HAHN, and
ELENI MANTIS MERCADER, *Administrative Patent Judges*.

KRIVAK, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

Appellants appeal under 35 U.S.C. § 134(a) from a non-final rejection of claims 18-48. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellants' claimed invention relates to a system for selecting a security format for data received over a network and converting the data according to the selected security format (Spec. ¶ [0024]).

Independent claim 18, reproduced below, is representative of the subject matter on appeal:

18. A system comprising:

> a network interface couplable with a public network to receive a first client message and first data that is encrypted according to a wireless security format and to receive a second client message and second data that is encrypted according to a wired security format;
>
> a selection system coupled with the network interface to select a first security format conversion for the first data and to select a second security format conversion for the second data; and
>
> a conversion system coupled with the selection system to perform the first security format conversion on the first wireless security format encrypted data and to perform the second security format conversion on the second wired security format encrypted data.

REFERENCE

Strahm	US 2002/0133598 A1	Sep. 19, 2002

The Examiner rejected claims 18-48 under 35 U.S.C. § 102(e) as anticipated by Strahm.

Appellants contend Strahm does not teach a network interface receiving a first client message and first data encrypted according to a wireless security format. Appellants also contend Strahm does not teach a

selection system or conversion system selecting and performing a first security format conversion on the wireless security format encrypted data. (App. Br. 10-11)[2]

ANALYSIS

With respect to independent claim 18, the Examiner finds Strahm teaches a mobile client connecting to a home agent after establishing a security protocol for the connection. In Strahm, Wireless Transport Layer Security (WTLS), a wireless encryption protocol, may be used as the security protocol, in addition to Transport Layer Security (TLS) or Secure Sockets Layer (SSL) (¶ [0024]; Ans. 5). The Examiner further finds Strahm teaches selecting a security protocol and performing decryption according to the selected protocol. "Thus a message encrypted according to WTLS at the first firewall would correspondingly be decrypted with the same algorithm at the second firewall for the home agent 160." (Ans. 5)

Appellants contend Strahm does not teach the home agent uses WTLS, or any other wireless security format (App. Br. 11, Reply Br. 3-4). Further, Appellants contend WTLS encrypted data would be converted to another format, such as the wired format SSL, before reaching Strahm's home agent. Thus, the home agent would not receive any WTLS encrypted data for decrypting according to a wireless security format. (App. Br. 12; Reply Br. 4) To bolster this argument Appellants note Strahm's Figure 7, which is a diagram of the home agent processing configuration, includes the label "TLS/SSL" and not WTLS (App. Br. 11-12; Reply Br. 4). Appellants

[2] Appellants' Brief (Second) filed May 9, 2008, is referenced throughout this opinion.

further assert the Examiner has not provided sufficient reasoning as to how WTLS data remains encrypted throughout its transversal from Strahm's mobile client through the Internet to the home agent (App. Br. 12). Appellants' arguments are not persuasive.

As found by the Examiner, Strahm discloses a system wherein a mobile client and home agent establish different security protocols for different connections, including WTLS (Strahm ¶¶ [0024], [0026]; Ans. 5). In addition, encrypted information is sent from the mobile client to the home agent through an established connection (Strahm ¶ [0034]). The Examiner asserts "Strahm is silent with regards to the appellants' assertion that the data encryption format would be converted on route to the home agent 160" (Ans. 5). Indeed, there is no suggestion in Strahm that WTLS encrypted data be decrypted or converted to another format before it reaches the home agent. The fact that Figure 7 only includes the label "TLS/SSL" does not detract from the affirmative disclosure of WTLS as a choice for security protocol for connecting between the mobile client and home agent (Strahm ¶ [0024]). Further, Appellants' suggestion that the Examiner must provide sufficient reasoning as to how WTLS data remains encrypted throughout its transversal from the mobile client to the home agent is without merit (App. Br. 12). There is no limitation in claim 18 regarding how data encrypted according to a wireless security format remains encrypted on route to the network interface.

Appellants' further argue Strahm's mobile client does not receive the claimed client messages with wireless security format encrypted data (App. Br. 12; Reply Br. 5-6). Although the Examiner "admits that the client sends messages to home agent 160, and does not receive its own messages," as

discussed above, the Examiner relies on Strahm sending WTLS encrypted data from the mobile client *to the home agent* where the WTLS encrypted data is decrypted, meeting the limitations of claim 18 (Ans. 5-6). Thus, Appellants' argument that the mobile client does not receive client messages is moot. Therefore, because Strahm teaches all of claim 18's limitations, Strahm anticipates claim 18, in addition to independent claims 29, 36, 40, and 47, and claims 19, 22-26, 31, 32, 35, 38, 39, and 42, which depend therefrom.

With respect to claims 27, 33, and 43-46, Appellants contend Strahm's mobile client does not disclose the respective claim limitations (App. Br. 14, 15; Reply Br. 8-9, 11). Further, Appellants assert, it is improper for the Examiner to rely on features of both the mobile client (for meeting the wireless security format limitation in independent claim 18) and the home agent (for meeting the dependent claim limitations) because this would require a modification of Strahm's disclosure (Reply Br. 9, 11). However, as noted above, the Examiner does not rely on the mobile client to meet the limitation of a wireless security format as recited in claim 18; the Examiner relies on Strahm's home agent receiving wireless security format encrypted data (Ans. 5). Therefore, Strahm teaches the limitations of claims 27, 33, and 43-46.

With respect to claims 28, 34, and 48, Appellants contend neither Strahm's home agent nor mobile client resides in a data center between a first switch within the data center and a second switch within the data center (App. Br. 15; Reply Br. 9-10). Appellants also assert it is improper for the Examiner to rely on features of both the mobile client (to meet the wireless security format limitation in independent claim 18) and the home agent (to

meet the data center limitation in dependent claim 28) because this would require a modification of Strahm's disclosure (Reply Br. 10). However, as noted above, the Examiner is relying on Strahm's home agent receiving wireless security format encrypted data (Ans. 5). Regarding the data center limitation, we agree with the Examiner's finding that Strahm's destination network comprises a data center, and that the claimed network device, i.e., the home agent, resides in the data center between firewall 152 (meeting the limitation of a first switch) and a connection to Intranet 150 that inherently requires a switch (meeting the limitation of a second switch) (Fig. 1; Ans. 4, 6). Therefore, Strahm teaches the limitations of claims 28, 34, and 48.

With respect to claims 20, 21, 30, 37, and 41, the Examiner finds port number 443 is an inherent port used by the SSL protocol, and using port numbers 9208 to 9282 for the wireless security format encrypted data is inherent "because these ports are well known to be unassigned" and are "a design choice" (Ans. 7). However, as Appellants assert, the Examiner has not provided a sufficient reason why port numbers 9208 to 9282 would be inherent (App. Br. 15). The fact that Appellants *may* choose to use certain port numbers does not anticipate the claimed port numbers. Therefore, Strahm does not anticipate claims 20, 21, 30, 37, and 41.

DECISION

The Examiner's decision rejecting claims 18, 19, 22-29, 31-36, 38-40, and 42-48 is affirmed.

The Examiner's decision rejecting claims 20, 21, 30, 37, and 41 is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED-IN-PART

kis

MISSION/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040